# SYSTEM AND METHOD FOR GENERATING PSEUDO-RANDOM NUMBERS

## Abstract of the Disclosure

A method and system is provided for generating pseudo-random numbers utilizing techniques of both the SHA-1 and DES encryption standards, wherein a pseudo-random number generator is re-keyed periodically using an external input of physical randomness. In accordance with one embodiment of the present invention, a current seed value $S_j$ is loaded from a non-volatile storage. Next, values E, representative of environmental randomness, and C, representative of configuration data are likewise loaded. A new seed value, $S_{j+1}$, is generated in accordance with the equation $S_{j+1} = f(S_j; A; C; E)$, wherein f represents a selected encryption algorithm , and B is a second constant, and wherein $S_j$ is concatenated with A, which is concatenated with C which is concatenated with E. The new seed is then written to the non-volatile storage. Next, a key, K, is generated in accordance with the equation $K = f(S_j; B; C; E)$, wherein B is a second constant. Lastly, a pseudo-random number output, $P_n$, is generated in accordance with the equation $P_n = f_{3DES}(K, P_{n-1})$, where $f_{3DES}$ represents the operation of triple DES encryption hardware, and $P_{n-1}$ is the previously generated pseudo-random number.